



DEPARTMENT OF THE NAVY

BUREAU OF MEDICINE AND SURGERY
WASHINGTON, D C 20372-5120

IN REPLY REFER TO

BUMEDINST 5530.1

BUMED-09B1

17 JUN 91

BUMED INSTRUCTION 5530.1

From: Chief, Bureau of Medicine and Surgery
To: All Internal BUMED Codes

Subj: PHYSICAL SECURITY, LOSS PREVENTION, AND ANTITERRORISM
PROGRAMS

Ref: (a) OPNAVINST 5530.14B
(b) SECNAVINST 5500.4F
(c) BUMEDINST 5500.1
(d) OPNAVINST 5510.1H
(e) NDWINST 5530.1A
(f) SECNAVINST 5214.2B

1. Purpose. To establish headquarters policy and provide procedures for implementing an effective physical security, loss prevention, and antiterrorism program at the Bureau of Medicine and Surgery (Potomac Annex) as directed by reference (a). References (b) through (e) are provided for additional guidance.

2. Cancellation. NAVMEDCOMINST 5530.3.

3. Scope. Applies to all buildings and grounds within the Potomac Annex and under the authority of the Chief, Bureau of Medicine and Surgery. Specific exemptions are made throughout this instruction for the tenant activity, but unless specifically stated as an exception, this instruction applies to the tenant activity regardless of tenancy.

4. Responsibility. Physical security is the responsibility of all military and civilian personnel assigned to this command.

a. MED-09B1 is the command security officer and is responsible for planning, implementing, enforcing, and supervising physical security, loss prevention, and antiterrorism programs for this command. The security officer is designated the antiterrorism officer.

b. All assistant chiefs and special assistants must ensure compliance with this instruction.

5. Review. This plan is reviewed annually and updated as necessary. Send recommendations for changes at any time to MED-09B1.

BUMEDINST 5530.1

17 JUN 91

6. Abbreviations. The following abbreviations are used in this instruction:

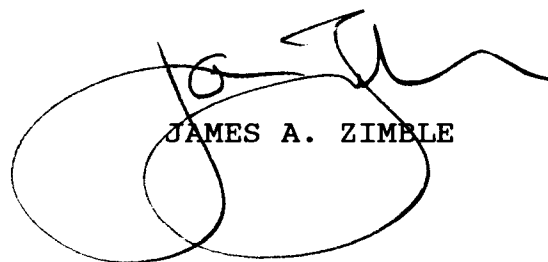
ADP	Automatic data processing
BUMED	Bureau of Medicine and Surgery
DoD	Department of Defense
EOD	Explosive Ordnance Disposal
FPS	Federal Protective Service
GSA	General Services Administration
LPS	Loss Prevention Subcommittee
M-L-S-R	Missing, Loss, Stolen, and Recovery
NSIC	Naval Security and Investigative Command
OOD	Officer of the Day
PSRB	Physical Security Review Board
PSRC	Physical Security Review Committee
THREATCON	Threat Conditions
CNO	Chief of Naval Operations

7. Forms

a. OF 7 (11-50), Property Pass is available from the BUMED Supply Room, Building Five, room 5000.

b. BUMED 8150/1 (3-91), Bomb Threat Report, and BUMED 5532/1 (9-90), Evacuation Search Chart, are stocked at the Information Desk, Building One, room 1104.

8. Reports Exemption. The requirements contained in this instruction are exempt from reports control by reference (f), part IV, paragraph G8.



JAMES A. ZIMBLE

17 JUN 91

CONTENTS

	Page
Chapter 1, Introduction	1
Definitions	1
Security Responsibilities	1-2
Organization	2
Chapter 2, Program Management	3
Physical Security Education and Training	3
Planning for Security Programs	3
Waivers and Exceptions	3
Security Priority Levels	3
Threat Analysis	3
Vulnerability	3
Chapter 3, Restricted Areas and Area Controls	5
Restricted Areas	5
Security Areas	5
Chapter 4, Personnel and Vehicle Access, Identification, and Movement	7
Purpose and Scope	7
Responsibility	7
Procedures	7-9
Admittance and Departure Requirements	7
Types of Authorized Identification	8
Acceptable Credentials from Other Agencies	8-9
Vehicle and Pedestrian Gate Hours of Operation	10

	Page
Chapter 5, Loss Prevention	11
Property Control	11
Key and Lock Control	11
Missing, Loss, Stolen, and Recovery Property Reporting (M-L-S-R)	11-12
Investigative Action	12
Controls and Coordination	12
Followup	12
Attachment 5A, Key and Lock Control	13
Purpose	13
Responsibility	13
Procedures	13
Minimum Standard Procedures	13-14
Duplication of Keys	14
Violations	14
Key Lock Boxes	14
Chapter 6, Physical Security Inspection Program	15
An Annual Physical Security Survey	15
Documentation and Reporting	15
Administrative Use	15
Corrective Action	15
Chapter 7, Combatting Terrorist Threat	17
Threat Conditions	17
Definitions	17
Procedural Guidance	17

	Page
Attachment 7A, Recommended Threatening Conditions (THREATCON) Measures	19-20
Attachment 7B, Bomb Threat Procedures	21
Attachment 7C, Evacuation Procedures	23
Attachment 7D, Procedures to be Followed Between BUMED and its Tenant Activity for Fires or Threats Against Personnel or Facilities	25

17 JUN 91

CHAPTER 1

INTRODUCTION

1. Definitions. The following definitions apply:

a. Physical Security. That part of security concerned with physical security measures designed to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against espionage, sabotage, damage, or theft.

b. Physical Security Survey. An indepth examination of the physical security of an activity to determine compliance with physical security policy. A physical security survey is conducted by the security officer or representative. Survey results are used as a management tool to improve physical security of the activity surveyed and to inform the Chief, BUMED of the physical security of the command.

c. Waiver. A written temporary relief, not to exceed 1 year, from specific physical security standards imposed by reference (a), pending actions or accomplishment of actions which results in conformance with the standards required. Interim compensatory physical security measures are required. Division directors and special assistants requiring waivers must submit their requests to the security officer who forwards it through the chain of command to Chief of Naval Operations (CNO) for approval.

d. Exceptions. An approved permanent deviation from a specific physical security provision of reference (a). Division directors and special assistants requiring exceptions must submit their requests to the security officer who forwards it through the chain of command to CNO for approval.

2. Security Responsibilities

a. Chief, Bureau of Medicine and Surgery is responsible for physical security at the Potomac Annex, for appointing a security officer, and for establishing and maintaining a physical security, loss prevention, and antiterrorism program within the command.

b. MED-09B1 is the security officer for BUMED. The security officer is responsible for determining the adequacy of the command's physical security, loss prevention, and antiterrorism programs; for identifying those areas in which improvements are required; and providing recommendations for improvements to the Chief, BUMED.

17 JUN 91

c. MED-09B12 is designated physical security specialist and is responsible for developing security requirements, policies, and procedures for the command.

3. Organization. Per reference (a), the Physical Security Program includes the following working groups:

a. Physical Security Review Committee (PSRC). The Deputy Chief, BUMED or designated officer (O-6 or above) acts as Chairman, PSRC. Membership must comply with the requirements of reference (a), and may include a representative of the Naval Security and Investigative Command (NSIC) or the Naval Protective Service (NPS). The PSRC must meet at least quarterly and will appoint a loss prevention subcommittee.

b. Loss Prevention Subcommittee (LPS). The LPS must meet quarterly and be chaired by the security officer. Membership must include the physical security specialist, a representative from the command evaluation section, and the fiscal and supply officer.

c. Physical Security Review Board (PSRB). The Chief, BUMED establishes the PSRB under the chairmanship of the Deputy Chief, BUMED. Membership must include the security officer, the physical security specialist, and the president of the tenant activity, or his or her representative. The PSRB must meet at least annually.

CHAPTER 2

PROGRAM MANAGEMENT

1. Physical Security Education and Training. The physical security specialist (MED-09B12) must develop and coordinate a command-wide physical security training program. The primary goal of this program is to raise the level of awareness of all personnel in the areas of:

- a. Physical security standards and procedures.
- b. Loss prevention.
- c. Identification and reporting of security violations.

2. Planning for Security Programs. The physical security specialist must develop the physical security, loss prevention, and antiterrorism plan per reference (a). The tenant's activity plan must be coordinated with the BUMED Security Officer.

3. Waivers and Exceptions. Any variance from required security criteria, temporary or permanent, requires a waiver or exception approved by higher authority. Waiver and exception requests must be sent per reference (a).

4. Security Priority Levels. BUMED physical security programs and resource priorities must be based on the most current threat analysis and vulnerability information. These priorities determine the urgency of need for completion of security projects, upgrades, etc.

- a. Protection of mission essential assets (communications equipment and Automatic Data Processing (ADP) equipment).

- b. Protection of valuable assets (recreational equipment and snack bar).

5. Threat Analysis. NSIC provides a threat analysis profile for Potomac Annex. NSIC updates the profile at least annually, and more often, if needed based on changing conditions. Classified reports are handled per reference (d).

6. Vulnerability. The NSIC threat analysis profile and physical security survey, along with other security inspection reports and security violation data, are used by the PSRC to determine the overall current vulnerability of the Potomac Annex, and to assist in establishing physical security program priorities.

CHAPTER 3

RESTRICTED AREAS AND AREA CONTROLS

1. Restricted Areas. The Chief, BUMED will designate restricted areas for BUMED assets. Two types of restricted areas exist:

a. Limited Area. An area which contains a security interest which if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission.

b. Controlled Area. An area which contains a security interest which if lost, stolen, or sabotaged would cause identifiable damage to the command mission.

2. Security Areas

a. The security areas are listed below. Areas designated as restricted areas are established by the Chief, BUMED "pursuant to lawful authority and promulgated pursuant to DoD Directive 5200.8, dated July 29, 1980 and section 21, Internal Security Act of 1950."

b. The following areas are designated as either limited or controlled areas:

<u>Building</u>	<u>Code</u>	<u>Room</u>	<u>Limited</u>	<u>Controlled</u>
1	09B12	1000	X	
		1015	X	
3	27	3000		X
3	27	3005		X

c. Potomac Annex is designated as a controlled area from 1830 to 0600 hours, 5 days a week, and 24 hours a day on Saturday, Sunday, and holidays. At all other times, the Potomac Annex is a non-restricted installation.

d. The following areas are non-restricted areas, but still areas of security interest and command responsibility which are listed by priority.

(1) Flag Quarters "AA," "BB," and "CC" (under jurisdiction of Washington Navy Yard Housing District).

(2) Building 3, Mail Room.

(3) All offices containing level II and level III ADP equipment (Zenith and VAX equipment).

(4) Rotunda, physical fitness equipment.

CHAPTER 4

PERSONNEL AND VEHICLE ACCESS, IDENTIFICATION, AND MOVEMENT

1. Purpose and Scope. To prescribe policy, procedures, and responsibilities for the access, movement, and identification of individuals employed, assigned, or visiting the Potomac Annex. This chapter is applicable to all persons entering, while on, or departing this compound.

2. Responsibility

a. The Department of Defense (DoD) Buildings Manager, Washington Navy Yard, is responsible for building security at the Potomac Annex.

b. The Federal Protective Service (FPS), General Services Administration (GSA) is responsible for providing normal protection for the buildings, Government property therein, and the safety of its occupants. Supplemental protection may be on a reimbursable basis.

c. The tenant activity is responsible for security of its assigned areas, to include, protection of personnel, equipment, and classified material within the confines of its respective areas.

3. Procedures

a. Admittance and Departure Requirements

(1) Authorized identification or escorts are required to gain admittance to and remain within the compound. Identification cards must be worn conspicuously on the outer garments while individuals are on the compound.

(2) During normal duty hours (0600-1830 hours), Monday through Friday, visitors who do not possess valid identification will be admitted only after verification from the office being visited. Visitors will be stopped and asked for the name of the person sponsoring their entry and which building is to be visited. The guard will call the appropriate security personnel to verify the access authorization before allowing the visitor to proceed. After verification, the visitor must sign the visitor's log, be issued a visitor's pass, and be directed to his or her destination. The visitor's pass must be turned in before the visitor departs the compound. Visitors are the responsibility of the office being visited.

(3) Vehicle admittance and exit requirements must be one of the following:

(a) A valid Potomac Annex vehicle pass or valid DoD vehicle decal displayed in or on the vehicle. All military and civilian drivers and passengers are required to show valid identification before entering the compound.

(b) Personnel not in possession of authorized identification must be required to show a valid photographic form of identification. The guard will check the photograph against the person for proper match. If there is a proper match, the driver or passenger, must sign in on the visitor's log and be issued a visitor's pass, after verification has been established using the procedures in section 3a(2). The pass must be turned in before departing the compound.

(c) Delivery personnel must display a bill of lading, shipping document, invoice, or DoD contract indicating delivery to the Potomac Annex. The guard will inspect the material to verify the documentation. The driver must display a valid photographic drivers license. After verification of proper match, the driver must sign in on the contractor's log and be issued a contractor's pass. The pass must be turned in before departing the compound.

(d) All vehicles entering or departing the Potomac Annex are subject to search and inspection by the guard or FPS.

b. Types of Authorized Identification

(1) Armed Forces of the United States - Green.

(2) Armed Forces of the United States - Red (United States Naval Reserves-Readiness (USNR-R)).

(3) Armed Forces of the United States - Gray (Retired USN, USMC, USA, USAF).

(4) Civil Service ID Card.

(5) Department of Defense Building Pass.

(6) United States Department of State Building Pass.

c. Acceptable Credentials from Other Agencies. Representatives of the following agencies may be admitted to the Potomac Annex at any time upon presentation of official credentials:

- (1) Federal Bureau of Investigation (FBI).
- (2) Military Intelligence (U.S. Army).
- (3) Naval Security and Investigative Command (NSIC).
- (4) U.S. Secret Service (Treasury Department).
- (5) Criminal Investigation Command (U.S. Army).
- (6) Defense Investigative Service (DIS).
- (7) General Services Administration (GSA).
- (8) C & P Telephone Company.
- (9) American Telephone & Telegraph Company.
- (10) Counterintelligence Credentials (USMC).
- (11) Central Intelligence Agency (CIA).

d. Vehicle and Pedestrian Gate Hours of Operation. Vehicle and pedestrian gate hours are:

<u>Gate and Location</u>	<u>Hours of Operation</u>
Post #1, "E" Street Gate	24 hours
Post #2, "C" Street Gate	0600 to 1830 Hours

Note: During security hours 1830 to 0600 hours, Monday through Friday, and 24 hours a day on Saturday, Sunday, and holidays, use "E" Street Gate only.

CHAPTER 5

LOSS PREVENTION

1. Property Control. Following references (b) and (c), Government property must be protected from loss or abuse by all reasonable means.

a. The removal of Government property not covered by a bill of lading, invoice, or supply receipt, and personal property not accompanied by proof of ownership may only be accomplished by means of a Property Pass (OF 7) signed by a division director, special assistant, the supply officer, or security manager.

b. All division directors and special assistants must develop internal control procedures to ensure adequate records of and accounting for all property.

c. Special Assistant for Command Evaluation (MED-09CE) conducts audits as directed to ensure the integrity of established controls and procedures to safeguard property.

d. Division directors and special assistants are responsible for the protection and accountability of all property under their control, and for the M-L-S-R property report.

2. Key and Lock Control. Attachment 5A of this chapter is a guide for BUMED in establishing a key and lock control program. The Facilities Manager (MED-09B23) is responsible for program management and supervision of the command key and lock program. Included within this program are all keys and locking devices used to protect or secure restricted areas and the compound perimeter.

3. M-L-S-R Property Reporting. Timely reporting is vital to the M-L-S-R tracking program. The security officer is the focal point for report monitoring. The LPS must review M-L-S-R property reports sent during any calendar month and forward to the Chairman, PSRC per reference (a).

a. Division directors and special assistants must ensure all personnel, in handling inventory, supplies, etc., are aware of M-L-S-R property reporting procedures in references (b) and (c).

b. On discovery of a suspected loss or theft, the property custodian makes a preliminary inquiry to determine if the property is, in fact, missing. If the property is missing, the property custodian must report the loss to the division director or special assistant.

c. The division director or special assistant appoints a survey officer to determine if an M-L-S-R property report and a survey are required. The survey officer must report back to the division director or special assistant within 1 working day.

d. Report losses within 2 working days of discovery. (See reference (b) for the definition of reportable losses). The initial report must include essential identification and a general description of the circumstances of loss and followup action being taken. Send the report to the security manager for review. The security manager will inform the Chairman, PSRC.

e. Send followup reports per reference (b).

4. Investigative Action. In addition to the division director's or special assistant's report of survey inquiry, the security officer must report all losses to the Federal Protective Service, Zone 1, 647-1814, and the Naval Security and Investigative Command, 433-3858, for further action, if necessary.

5. Controls and Coordination

a. Forward draft copies of all reports of losses, theft, and vandalism to the security officer to determine if M-L-S-R property reporting is required. If it is required, establish a suspense of 10 working days and return the draft to the division director or special assistant for the appropriate action.

b. If a copy is not received by the security officer by the established suspense date, it is a late report. An additional 10 working days may be granted to send the report. If the division director or special assistant fails to meet the above deadline, he will be required to submit the report to the security manager within 5 working days of the final notice with a written explanation for the delay.

6. Followup. The security officer makes quarterly analyses of M-L-S-R property dollar loss figures in comparison to the accumulated security violation reports for the quarter to determine if there are corresponding risk patterns. Forward these analyses to the division director or special assistant with recommendations for corrective action. The security officer sends the above analyses, via the LPS, to the PSRC for coordination of security upgrades.

ATTACHMENT 5A

KEY AND LOCK CONTROL

1. Purpose. To establish procedures and guidance for implementing an effective key and lock control program for BUMED.

2. Responsibility. The Facilities Manager (MED-09B23) is designated key and lock control officer for BUMED and is responsible for establishing an effective key and lock program. This includes all keys, locks, and locking devices used to protect or secure restricted areas, activity perimeter, security facilities, critical assets, or sensitive supplies. Not included in this program are keys, locks, and locking devices used for convenience, privacy, or administrative personal purposes. Classified material is handled following reference (d), and is the responsibility of the security officer.

3. Procedures

a. The key and lock control officer must develop standard procedures for key and lock control for the command, and must conduct semiannual inventories to ensure all issued keys and locks are accounted for and appropriate standards are met in the control of locking devices. A written record of each inventory must be kept with the key issue log and a copy forwarded to the security office for filing.

b. The key issue log shows keys onhand, keys issued, to whom, date or time, and signature of person issuing and receiving keys. Persons who sign for keys are responsible for them at all times, until they are returned.

c. Division directors and special assistants must ensure that all keys and locking devices within their spaces are in good operating condition. Report bent or broken keys and locking devices which are inoperable, defective, or excessively rusted to the Facilities Manager for appropriate action.

4. Minimum Standard Procedures

a. Following reference (a), rotate padlocks or changeable cores at least annually. Change locks immediately when compromised or when any person with access to the key or combination is transferred or found unreliable. This may be accomplished by the key and lock control officer.

b. Keys must not be left in locks at any time. Relock open padlocks to the staple or other immovable object to allow use of doors or openings, or secure in a locked key control box or safe. Do not store padlocks with shackle open or key inserted. Do not carry padlocks on your person.

BUMEDINST 5530.1
17 JUN 91

c. All locking devices used for low, medium, or high security applications must meet military specifications for the appropriate levels of security.

5. Duplication of Keys

a. Controlled keys may be duplicated only through written request and approval by the responsible division director or special assistant. Requests must include the key number, identity of the secured division involved, the number of duplications needed, and reason for duplication. Forward the request to the key and lock control officer, via the physical security specialist.

b. Inventory and issue all duplicated keys following the established written key control guidelines.

6. Violations. Report lost, damaged, or misplaced keys or locking devices, or any suspected compromise or breach, to the key and lock control officer, who will immediately record all incidents and report them to the security officer. If there are signs of forced entry or actual attempted theft, notify the FPS at 647-1814.

7. Key Lock Boxes. Approved key security boxes are available through the normal supply channels.

CHAPTER 6

PHYSICAL SECURITY INSPECTION PROGRAM

1. An Annual Physical Security Survey is conducted by the physical security specialist. The results of this survey are kept on file for 2 years. The physical security specialist must send a copy of the survey to the security officer for review and consideration.
2. Documentation and Reporting. The physical security specialist conducts the annual security survey using the checklist in reference (a). Use completed checklists to monitor corrective actions.
 - a. Initial Report. Following reference (a), the physical security specialist must complete a written report of findings and recommendations within 30 days of completion of survey, and forward a copy to the division directors or special assistants concerned.
 - b. Monitoring Reports. The physical security specialist must provide updates to the respective division directors or special assistants on all items identified during the survey which have not yet been corrected. The first report addresses each specific finding and specifies corrective action and tentative completion date of each. Successive reports may list corrected items as complete. Delete items from subsequent reports until all items are complete. Forward copies of all reports to the security officer.
3. Administrative Use. Reports generated by the security survey are used to determine requirements for upgrading local security measures and programs. Do not forward to higher authority. Use of these reports by the tenant activity is subject to requirements of the respective command.
4. Corrective Action. Security standards set by higher authority must be met whenever possible and practical to do so. Waiver and exception requests are sent, via the security officer, for any requirement which cannot be met.

CHAPTER 7

COMBATTING TERRORIST THREAT

1. Threat Conditions. Reference (e) establishes threat conditions (THREATCONS) and suggests measures for those THREATCONS.

2. Definitions. THREATCONS are defined as follows:

a. THREATCON ALPHA. This condition is declared as a general warning of possible terrorist activity, the nature and extent of which are unpredictable, when the circumstances do not justify full implementation of the measures contained in THREATCON BRAVO. It may be necessary to implement selected measures from THREATCON BRAVO. The measures in this THREATCON must be capable of being maintained indefinitely.

b. THREATCON BRAVO. This condition is declared when there is an increased and more predictable threat of terrorist activity even though no particular target has been identified.

c. THREATCON CHARLIE. This condition is declared when an incident occurs or when intelligence is received indicating that some form of terrorist action is imminent.

d. THREATCON DELTA. This condition applies in the immediate area where a terrorist attack has occurred or when intelligence received indicates terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

3. Procedural guidance for THREATCONS, bomb threats, fire, or evacuation of personnel assigned to the Potomac Annex are contained in attachments 7A, 7B, 7C, and 7D.

ATTACHMENT 7A

RECOMMENDED THREATCON MEASURES

1. THREATCON ALPHA

a. Measure 1. At regular intervals, remind all personnel to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; be alert for unidentified vehicles on, or in, the vicinity of naval installations; and be alert for abandoned parcels or suitcases or any unusual activity.

b. Measure 2. Keep available at all times the security officer or other appointed personnel, who have access to plan for evacuating buildings and areas in use and for sealing off any areas where an explosion or attack has occurred. Keep available all key personnel who may be needed to implement security plans.

c. Measure 3. Secure buildings, rooms, and storage areas not in regular use.

d. Measure 4. Increase security spot checks of vehicles and persons entering the installation and nonclassified areas under the jurisdiction of the installation commander.

e. Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

2. THREATCON BRAVO

a. Measure 6. Keep all personnel involved in implementing antiterrorist contingency plans on call.

b. Measure 7. Where possible, cars and such objects as crates, trash containers, etc., are to be moved at least 80 feet (25 meters) from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

c. Measure 8. Examine all mail for letter or parcel bombs. (This examination is increased above normal).

d. Measure 9. Make staff aware of the general situation to stop rumors and prevent unnecessary alarm.

e. Measure 10. At an early stage, inform local security committees of any action being taken and why.

f. Measure 11. Physically inspect command visitors and a percentage of their suitcases, parcels, and other constraints.

BUMEDINST 5530.1

17 JUN 91

3. THREATCON CHARLIE

a. Measure 12. Continue all THREATCON BRAVO measures or introduce those outstanding.

b. Measure 13. Keep available, at their place of duty, all personnel who are responsible for implementing antiterrorist plans.

c. Measure 14. Limit access points to an absolute minimum.

d. Measure 15. Strictly enforce control at entry and search a percentage of vehicles.

e. Measure 16. Erect barriers and obstacles to control traffic flow.

4. THREATCON DELTA. Measure 17. Continue or introduce all measures listed in THREATCON BRAVO and CHARLIE.

ATTACHMENT 7B

BOMB THREAT PROCEDURES

1. Upon receipt of a bomb threat:
 - a. During working hours: immediately notify MED-09B and MED-09B1. MED-09B has authority to evacuate buildings.
 - b. During security hours: immediately notify the Officer of the Day (OOD). The OOD has authority to evacuate buildings.
2. MED-09B personnel or duty personnel must then:
 - a. Notify the Federal Protective Service: 708-1111.
 - b. Notify the Bomb Disposal Team: Military 9-911 or Fort McNair: 475-1988.
 - c. Use the Bomb Threat Report, BUMED 8150/1, to ascertain as much information as possible.
 - d. If an evacuation is directed, use the Evacuation Search Chart, BUMED 5532/1, as a guide. During the search, if any suspicious or unknown packages or devices are found, **DO NOT TOUCH**. Report findings to the explosive ordnance disposal (EOD) personnel when they arrive.

ATTACHMENT 7C

EVACUATION PROCEDURES

1. On report of a bomb threat, immediately notify the FPS. Stay on the line until instructed otherwise by the FPS.
2. Initiate established evacuation procedures including:
 - a. If a telephone threat, the senior person in the area should work with the person receiving the call to gather as much information as possible.
 - b. Before leaving the building, the senior person should check to ensure all others have left the building; ensure all classified documents and equipment are properly secured; and ensure all perimeter doors and windows are left open.
 - c. Upon leaving the building, post persons at a safe distance from the building where they can observe anyone entering or leaving. Go to a designated gathering place and check to ensure all persons are accounted for.
 - d. Do not re-enter the building until it has been released by responding FPS and EOD personnel. Report any persons entering the building after evacuation or failing to leave.
3. FPS Response. On notification of a bomb threat, the FPS notifies EOD, giving all available information.

ATTACHMENT 7D

PROCEDURES TO BE FOLLOWED BETWEEN BUMED AND
ITS TENANT ACTIVITY FOR FIRES OR THREATS AGAINST
PERSONNEL OR FACILITIES

1. Discussion. If there is a threat against personnel or facilities at the Potomac Annex, or a fire or other emergency, the office receiving the threat or having the fire or other emergency must immediately notify the General Services Administration Control Center, 708-1111 and the BUMED Information Desk. The person covering the Information Desk will assume responsibility for notifying the occupants of the quarters at the Potomac Annex, the Board of Inspection and Survey (Building 6 occupants), and Navy Department offices or duty officers, as required. The tenant activity will notify higher echelon as required.
2. Procedures. After appropriate notifications required by the threat, fire, or other emergency have been made by the cognizant office, that office must notify the Information Desk at 653-1327/28 and provide all details pertinent to the threat, fire, or other emergency and provide all details of emergency response teams onboard, enroute, or assistance required.
3. Review and Renewal. These procedures are to be reviewed as necessary, but at least annually.